EPITECH. TECHNOLOGY

VIROLOGY

HANDLE WITH CARE

VIROLOGY

You're hired at *WePwnzU.co*, an offensive security company. You work solely on aggressive pen-testing and have been tasked to form a team and write a new offensive intrusion tool: *s0P0wn3d*.

Your team is specialized in covert intrusion to test the reactivity of SOC in large companies.

As such, the first and foremost quality of the tool you will write is **discretion**, it must be invisible to any and all Anti-Virus and monitoring solutions today and as inconspicuous to the naked eye.

You must not launch an attack of any kind against a target that has not given express and written consent as per the laws applicable to all parties.
Breaking the law can cost you both money and years. Breaching a company's trust can cost you your image, your current and future jobs. This is no joke, folks.

Some intrusions may last for long: *s0P0wn3d* must be as **resilient** as possible.

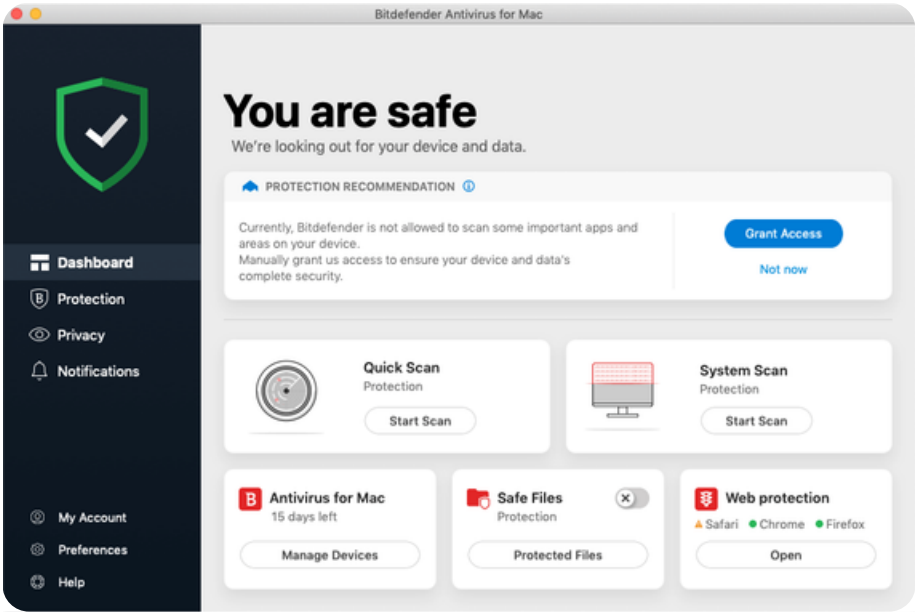
It will act as your central hub to manage the infected assets for the current intrusion's scope. It must be designed to assist you in your daily intrusion tasks:

- ✓ **spawning a shell** ;
- ✓ **creating a tunnel** ;
- ✓ **extracting credentials** ;
- ✓ and lots more.

Remember that **discretion** is key and the less fingerprint you leave, the better.

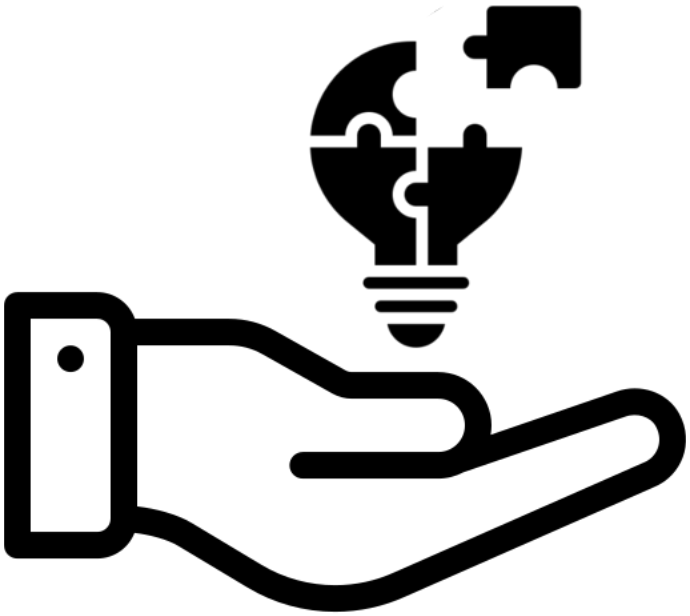
You are expected to write a fully functional working tool AND to test it [live] on multiple machines, with Windows operating systems.

The infection vector is not important here.
Your initial payload will be launched both from a limited account and an administrator account to evaluate how well it fares when given some or all access rights.



Once the discretion and resilience are assured, and once you can assure *s0P0wn3d* is efficient on the previouly mentionned tasks, enrich it with any of the following features:

- ✓ Keylogging ;
- ✓ RDP ;
- ✓ Cracking ;
- ✓ Pass-The-hash ;
- ✓ Extract sensitive files (keepass, SSH keys, config files,…) ;
- ✓ Phishing automation ;
- ✓ Horizontal propagation ;
- ✓ (Semi-) Automatic detection / exploit capabilities ;
- ✓ Userland syscalls (notably *fork* and *exec*) ;
- ✓ Pseudo-shell relying only on builtins to avoid exec / commands monitoring ;
- ✓ …



You are free to use any low-level library (cryptography, network, UI, …).
For discretion sake, you must not use any tool that automates any of *s0P0wn3d*'s main task (metasploit & co, mimikatz & co, empire, TheFatRat, …) but build your own tool.

To find a virtual machine for this project, have a look here, here or there for instance.
To build an Active Directory, you can follow these steps

v 1.0